

119 Dorothy Drive  
North Haledon, NJ 07508

Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

I am writing to voice my concern over the proposed rule changes to the amateur services that would allow encryption of wireless networking.

The amateur service relies on self policing. Because of this, the FCC can keep a low profile presence and a smaller budget requirement when viewed against the benefits of amateur radio to society. By allowing encryption, the ability of the ham community to self-police will be weakened and the burden of regulating any issues will fall back to the FCC.

The argument that medical information ( or other sensitive personal details ) would need to be encrypted does make sense. I would hate to be affected by a natural disaster, spend months recovering, only to then find my identity had been stolen when my SSN had been transmitted by volunteers. But, I strongly believe that encrypting the wireless physical layer is the wrong approach.

If you keep the wireless network unencrypted, how can you securely transfer medical and personal information? One idea is to have the data encrypted in a file by the hospital or OEM. This would leave the operation of the wireless network, and it's Part 97 operation, within the legal requirements. Instead of blanket encryption, the FCC could allow the transmission of encrypted payloads by government, state, or medial authorities. Part 97 operations would continue in the clear and all users would recognize certain encrypted files containing patient lists, etc. would be sent as a file. Encrypted by and decrypt-able only by the authorities.

It is important to understand the difference between full communications system encryption and the encryption of a file. I urge you to do some basic reading on how PGP operates. Basically, you would have a private key file and a public key file. Your private key file is what you use, with software ([GNUPG](#), for example) with a recipients public key file to encrypt a file. This encrypted file is now unreadable by even the sender. Only the intended recipient can decrypt the file by using his private key file and the senders public key.

Full wireless network encryption, however, would require much a more involved setup of all connected users, more training time for volunteers, and some sort of audit by hospitals and government users before their legal team would allow this data to flow. By keeping the encryption in their hands, amateur radio operators can continue to do what they do best, passing messages and data at a moments notice.

I would like to see some level of encryption being allowed in amateur communications for HIPAA requirements. Not only will encryption at the lowest level undermine the principals of amateur radio but the logistics of keeping an entire network running alone is difficult. Adding to that, the work needed to get all users setup with the encryption pass-phrases, etc. will add a level of difficulty that has historically been the reason commercial and government networks can't deploy as readily as amateur radio. Keep amateur radio unencrypted and allow for the transmission of encrypted files during emergencies, drills, and testing.

Sincerely Yours,

Peter Barletto  
KB2JAQ